The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity : Extended Abstract (Theoretical Computer Science and its Applications)

AUTHOR(S):

Hayashi, Ryotaro; Tanaka, Keisuke

数理解析研究所講究録 1426 巻 2005 年 64-70

Sampling Twice テクニックと匿名性をもつ RSA 暗号方式 (Extended Abstract)

The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity (Extended Abstract)

林 良太郎* 田中 圭介*
Ryotaro Hayashi Keisuke Tanaka

東京工業大学 数理・計算科学専攻
Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology

Summary— We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. To construct the schemes with anonymity, it is necessary that the space of ciphertexts or signatures is common to each user. In this paper, we focus on the techniques which can be used to obtain this anonymity property, and propose a new technique for obtaining the anonymity property on RSA-based cryptosystem, which we call "sampling twice." It generates the uniform distribution over $[0, 2^k)$ by sampling the two elements from $\mathbb{Z}_N$ where $|N| = k$. Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature, which have some advantages to the previous schemes.

Keywords: RSA, anonymity, encryption, undeniable and confirmer signature, ring signature.

1 Introduction

1.1 Background

We say that an encryption scheme or a signature scheme provides anonymity when it is infeasible to determine which user generated a ciphertext or a signature. A simple observation that seems to be folklore is that standard RSA encryption, namely, a ciphertext is $x^e \bmod N$ where x is a plaintext and (N, e) is a public key, does not provide anonymity, even when all moduli in the system have the same length. Suppose an adversary knows that the ciphertext y is created under one of two keys (N_0, e_0) or (N_1, e_1), and suppose $N_0 \leq N_1$. If $y \geq N_0$ then the adversary bets it was created under (N_1, e_1), else the adversary bets it was created under (N_0, e_0). It is not hard to see that this attack has non-negligible advantage. To construct the schemes with anonymity, it is necessary that the space of ciphertexts is common to each user. We can say the same thing about RSA-based signature schemes.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a new security requirement of the encryption schemes called "key-privacy" or "anonymity." It asks that the encryption provide (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. In [1], they provided the key-privacy encryption scheme, RSA-RAEP, which is a variant of RSA-OAEP, and made the space of ciphertexts common to each user by repeating the evaluation of the RSA-OAEP permutation $f(x, r)$ with plaintext x and random r, each time using different r until the value is in the safe range. For deriving a value in the safe range, the number of the repetition would be very large (the value of the security parameter). In fact, their algorithm can fail to give a desired output with some (small) probability.

Chaum and Antwerpen provided undeniable signature which cannot be verified without the signer's cooperation. The validity or invalidity of an undeniable signature can be ascertained by conducting a protocol with the signer, assuming the signer participates. Chaum provided confirmer signature which is undeniable signature where signatures may

* Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 14780190, 16092206.

	Sampling Twice	Repeating	Expanding	RSACD
Encryption	**this paper**	Bellare et al.	-	Hayashi et al.
Undeniable and Confirmer Signature	**this paper**	-	Galbraith et al.	-
Ring Signature	**this paper**	-	Rivest et al.	Hayashi et al.

Figure 1: The previous and our proposed schemes

also be verified by interacting with an entity called the confirmer who has been designated by the signer. Galbraith and Mao proposed a new security notion for undeniable and confirmer signature named "anonymity" in [5]. We say that an undeniable or confirmer signature scheme provides anonymity when it is infeasible to determine which user generated the message-signature pair. In [5], Galbraith and Mao provided the undeniable and confirmer signature scheme with anonymity. They made the space of signatures common to each user by applying a standard RSA permutation to the signature and expanding it to the common domain $[0, 2^{2k})$ where N is a public key for each user and $|N| = k$. This technique was proposed by Desmedt [3].

Rivest, Shamir, and Tauman [8] proposed the notion of ring signature, which allows a member of an ad hoc collection of users S to prove that a message is authenticated by a member of S without revealing which member actually produced the signature. Unlike group signature, ring signature has no group managers, no setup procedures, no revocation procedures, and no coordination. The signer does not need the knowledge, consent, or assistance of the other ring members to put them in the ring. All the signer needs is knowledge of their regular public keys. They also proposed the efficient schemes based on RSA and Rabin. In their RSA-based scheme, the trap-door RSA permutations of the various ring members will have ranges of different sizes. This makes it awkward to combine the individual signatures, so one should construct some trap-door one-way permutation which has a common range for each user. Intuitively, in the ring signature scheme, Rivest, Shamir, and Tauman solved this problem by encoding the message to an N_i-ary representation and applying a standard RSA permutation f to the low-order digits where N_i is a public key for each user. This technique is considered to be essentially the same as that by Desmedt. As mentioned in [8], for deriving a secure permutation g with a common range, the range of g would be 160 bits larger than that of f.

Hayashi, Okamoto, and Tanaka [6] recently proposed the RSA family of trap-door permutations with a common domain denoted by RSACD. They showed that the θ-partial one-wayness of RSACD is equivalent to the one-wayness of RSACD for $\theta > 0.5$, and that the one-wayness of RSACD is equivalent to the one-wayness of RSA which is the standard RSA family of trap-door permutations. They also proposed the applications of RSACD to encryption and ring signature schemes. Their schemes have some advantages to the previous schemes.

1.2 Our Contribution

In this paper, we focus on the techniques which can be used to obtain the anonymity property.

From the previous results mentioned above, we can find three techniques, repeating, expanding, and using RSACD, for anonymity of cryptosystems based on RSA.

Repeating Repeating the evaluation of the encryption (respectively the signing) with plaintext x (resp. message m), random r, and the RSA function, each time using different r until the value is smaller than any public key N of each user.
Bellare, Boldyreva, Desai, and Pointcheval used this technique for encryption scheme [1].

Expanding Doing the evaluation of the encryption (respectively the signing) with plaintext x (resp. message m), random r, and the RSA function, and expanding it to the common domain.
This technique was proposed by Desmedt [3]. In [5], Galbraith and Mao used this technique for the undeniable signature scheme. In [8], Rivest, Shamir, and Tauman also used this technique for the ring signature scheme.

RSACD Doing the evaluation of the encryption (respectively the signing) with plaintext x (resp. message m), random r, and the RSACD function.
In [6], Hayashi, Okamoto, and Tanaka proposed the RSACD function and applications of this function.

In this paper, we propose a new technique for obtaining the anonymity property of RSA-based cryptosystems. We call this technique "sampling twice." In our technique, we employ an algorithm `ChooseAndShift`. It takes two numbers $x_1, x_2 \in$

$\mathbb{Z}_N$ as input and returns a value $y \in [0, 2^k)$ where $|N| = k$, and if x_1 and x_2 are independently and uniformly chosen from $\mathbb{Z}_N$ then y is uniformly distributed over $[0, 2^k)$.

Sampling Twice Doing the evaluation of the encryption (respectively the signing) twice with plaintext x (resp. message m), random r_1 and r_2, and the RSA function, and applying our proposed algorithm `ChooseAndShift` for the two resulting values.

Then, by applying the sampling twice technique, we construct the schemes for encryption, undeniable and confirmer signature, and ring signature (See Figure 1.).

We summarize the (dis)advantage of our proposed schemes.

Our proposed encryption scheme with sampling twice is efficient with respect to the size of ciphertexts and the decryption cost. It is also efficient with respect to the encryption cost in the worst case. On the other hand, that in the average case is larger than those of the previous schemes. More precisely, in our encryption scheme, the number of modular exponentiations to encrypt in the average case is 2, while those in the previous schemes are 1 or 1.5.

Our proposed undeniable and confirmer signature scheme with sampling twice is efficient with respect to the size of signatures. On the other hand, the number of modular exponentiations for signing and that of computation of square roots are always 2, while those of the other schemes are 1 or 1.5 in the average case.

Our proposed ring signature scheme with sampling twice is efficient with respect to the size of signatures and the verification cost. On the other hand, the signing cost of our scheme is larger than those of the previous schemes in the average case.

If we use the RSACD function, the resulting value is calculated by applying the RSA function either once or twice. Fortunately, since applying the RSA function twice does not reduce security, we can prove that the RSACD function is one-way if the RSA function is one-way. Generally speaking, a one-way function does not always have this property, and we cannot construct a one-way function with a common domain.

On the other hand, in the sampling twice, repeating, and expanding techniques, the resulting value is calculated by applying the RSA function once. Therefore, it might be possible to apply these techniques to other one-way functions and prove the security of the resulting schemes.

The organization of this paper is as follows. In Section 2, we review the definitions concerning families of functions and the standard RSA family. We construct the algorithm `ChooseAndShift` and propose the sampling twice technique in Section 3. In Section 4, we propose the encryption schemes with anonymity. We conclude in Section 5.

Due to lack of space, details have been omitted from this paper. See the full version [7].

2 Preliminaries

We describe the definitions of families of functions, families of trap-door permutations, and θ-partial one-way.

Definition 1 (families of functions, families of trap-door permutations). *A family of functions $F = (K, S, E)$ is specified by three algorithms. The randomized key-generation algorithm K takes as input a security parameter k and returns a pair (pk, sk) where pk is a public key and sk is an associated secret key (In cases where the family is not trap-door, the secret key is simply the empty string.). The randomized sampling algorithm S takes pk and returns a random point in a set that we call the domain of the function and denote by $\mathrm{Dom}_F(pk)$. The deterministic evaluation algorithm E takes pk and $x \in \mathrm{Dom}_F(pk)$ and returns an output we denote by $E_{pk}(x)$. We let $\mathrm{Rng}_F(pk) = \{E_{pk}(x) \mid x \in \mathrm{Dom}_F(pk)\}$ denote the range of the function.*
We say that F is a family of trap-door permutations if $\mathrm{Dom}_F(pk) = \mathrm{Rng}_F(pk)$, E_{pk} is a bijection on this set, and there exists a deterministic inversion algorithm I that takes sk and $y \in \mathrm{Rng}_F(pk)$ and returns $x \in \mathrm{Dom}_F(pk)$ such that $E_{pk}(x) = y$.

Definition 2 (θ-partial one-way). *Let $F = (K, S, E)$ be a family of functions. Let $b \in \{0, 1\}$ and $k \in \mathbb{N}$. Let $0 < \theta \leq 1$ be a constant. Let A be an adversary. We consider the following experiments:*

Experiment $\mathbf{Exp}^{\theta\text{-pow-fnc}}_{F,A}(k)$
  $(pk, sk) \leftarrow K(k)$; $x \xleftarrow{R} \mathrm{Dom}_F(pk)$; $y \leftarrow E_{pk}(x)$
  $x_1 \leftarrow A(pk, y)$ where $|x_1| = \lceil \theta \cdot |x| \rceil$
  if $(E_{pk}(x_1 || x_2) = y$ for some $x_2)$ return 1
  else return 0

We say that the family F is θ-partial one-way if

$$\Pr[\mathbf{Exp}^{\theta\text{-pow-fnc}}_{F,A}(k) = 1]$$

is negligible for any adversary A whose time complexity is polynomial in k.

The "time-complexity" is the worst case execution time of the experiment plus the size of the code of the adversary, in some fixed RAM model of computation.

Note that when $\theta = 1$ the notion of θ-partial one-wayness coincides with the standard notion of

one-wayness. We say that the family F is one-way when F is 1-partial one-way.

We describe the standard RSA family of trap-door permutations denoted by RSA.

Definition 3 (the standard RSA family of trap-door permutations). *The standard RSA family of trap-door permutations* $\mathsf{RSA} = (K, S, E)$ *is as follows. The key generation algorithm takes as input a security parameter* k *and picks random, distinct primes* p, q *in the range* $2^{\lceil k/2 \rceil - 1} < p, q < 2^{\lceil k/2 \rceil}$ *and* $2^{k-1} < pq < 2^k$. *It sets* $N = pq$ *and picks* $e, d \in \mathbb{Z}^*_{\phi(N)}$ *such that* $ed = 1 \pmod{\phi(N)}$ *where* $\phi(N) = (p-1)(q-1)$. *The public key is* N, e, k *and the secret key is* N, d, k. *The sets* $\mathrm{Dom}_{\mathsf{RSA}}(N, e, k)$ *and* $\mathrm{Rng}_{\mathsf{RSA}}(N, e, k)$ *are both equal to* $\mathbb{Z}^*_N$. *The evaluation algorithm* $E_{N,e,k}(x) = x^e \bmod N$ *and the inversion algorithm* $I_{N,d,k}(y) = y^d \bmod N$. *The sampling algorithm returns a random point in* $\mathbb{Z}^*_N$.

In [4], Fujisaki, Okamoto, Pointcheval, and Stern showed that the θ-partial one-wayness of RSA is equivalent to the one-wayness of RSA for $\theta > 0.5$.

3 The Sampling Twice Technique

In this section, we propose a new technique for obtaining the anonymity property of RSA-based cryptosystems. We call this technique "sampling twice." In our technique, we employ the algorithm `ChooseAndShift`. It takes two numbers $x_1, x_2 \in \mathbb{Z}_N$ as input and returns a value $y \in [0, 2^k)$ where $|N| = k$.

```
Algorithm ChooseAndShift_{N,k}(x_1, x_2)
  if (0 ≤ x_1, x_2 < 2^k − N)
    return { x_1      with prob. 1/2
           { x_1 + N  with prob. 1/2
  elseif (2^k − N ≤ x_1, x_2 < N)
    return x_1
  else
    y_1 ← min{x_1, x_2};  y_2 ← max{x_1, x_2}
    return
      { y_1      with prob. (1/2 + N/2^{k+1}) × 1/2
      { y_1 + N  with prob. (1/2 + N/2^{k+1}) × 1/2
      { y_2      with prob. 1/2 − N/2^{k+1}
```

Note that $2^{k-1} < N < 2^k$ ensures $2^k - N < N$, $0 < \frac{1}{2} - \frac{N}{2^{k+1}} < 1$, and $0 < \frac{1}{2} + \frac{N}{2^{k+1}} < 1$. In order to run this algorithm, it is sufficient to prepare only $k + 3$ random bits.

We prove the following theorem on the property of `ChooseAndShift`.

Theorem 1. *If* x_1 *and* x_2 *are independently and uniformly chosen from* $\mathbb{Z}_N$ *then the output of the above algorithm is uniformly distributed over* $[0, 2^k)$.

Proof. To prove this theorem, we show that if x_1 and x_2 are independently and uniformly chosen from $\mathbb{Z}_N$ then $\Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z] = 1/2^k$ for any $z \in [0, 2^k)$. For any $z \in [0, 2^k - N)$, we have

$$\begin{aligned}
&\Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z] \\
&= \Pr[x_1 = z \ \wedge\ 0 \le x_2 < 2^k - N] \times \tfrac{1}{2} \\
&\quad + \Pr[(x_1 = z \ \wedge\ 2^k - N \le x_2 < N) \vee \\
&\qquad\qquad (x_2 = z \ \wedge\ 2^k - N \le x_1 < N)] \\
&\qquad\qquad \times (\tfrac{1}{2} + \tfrac{N}{2^{k+1}}) \times \tfrac{1}{2} \\
&= \tfrac{2^k - N}{N^2} \times \tfrac{1}{2} + \tfrac{2N - 2^k}{N^2} \times 2 \times (\tfrac{1}{2} + \tfrac{N}{2^{k+1}}) \times \tfrac{1}{2} \\
&= \tfrac{1}{2^k}.
\end{aligned}$$

It is clear that $\Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z'] = \Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z' + N]$ for any $z' \in [0, 2^k - N)$. Therefore, for any $z \in [N, 2^k)$, we have $\Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z] = 1/2^k$.

Furthermore, for any $z \in [2^k - N, N)$, we have

$$\begin{aligned}
&\Pr[\mathtt{ChooseAndShift}_{N,k}(x_1, x_2) = z] \\
&= \Pr[x_1 = z \ \wedge\ 2^k - N \le x_2 < N] \\
&\quad + \Pr[(x_1 = z \ \wedge\ 0 \le x_2 < 2^k - N) \vee \\
&\qquad (x_2 = z \ \wedge\ 0 \le x_1 < 2^k - N)] \times (\tfrac{1}{2} - \tfrac{N}{2^{k+1}}) \\
&= \tfrac{2N - 2^k}{N^2} + \tfrac{2^k - N}{N^2} \times 2 \times (\tfrac{1}{2} - \tfrac{N}{2^{k+1}}) = \tfrac{1}{2^k}.
\end{aligned}$$

□

By using the algorithm `ChooseAndShift`, we propose a new technique for obtaining the anonymity property. We call this technique "sampling twice."

Sampling Twice Doing the evaluation of the encryption (respectively the signing) twice with plaintext x (resp. message m), random r_1 and r_2, and the RSA function, and applying our proposed algorithm `ChooseAndShift` for the two resulting values.

4 Encryption

4.1 Definitions

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that the encryption provide (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. In [1], a public-key encryption scheme with common-key generation is described as follows.

Definition 4. *A public-key encryption scheme with common-key generation* $\mathcal{PE} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *consists of four algorithms. The common-key generation algorithm* $\mathcal{G}$ *takes as input a security parameter* k

and returns some common key I. The key generation algorithm $\mathcal{K}$ is a randomized algorithm that takes as input a common key I and returns a pair (pk, sk) of keys, a public key and a matching secret key. The encryption algorithm $\mathcal{E}$ is a randomized algorithm that takes the public key pk and a plaintext x to return a ciphertext y. The decryption algorithm $\mathcal{D}$ is a deterministic algorithm that takes the secret key sk and a ciphertext y to return the corresponding plaintext x or a special symbol $\perp$ to indicate that the ciphertext was invalid.

In [1], they formalized the property of "key-privacy." This can be considered under either the chosen-plaintext attack or the chosen-ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. (IK means "indistinguishability of keys.")

Definition 5 (IK-CPA, IK-CCA [1]). *Let $\mathcal{PE} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $b \in \{0,1\}$ and $k \in \mathbb{N}$. Let $A_{\text{cpa}} = (A^1_{\text{cpa}}, A^2_{\text{cpa}})$, $A_{\text{cca}} = (A^1_{\text{cca}}, A^2_{\text{cca}})$ be adversaries that run in two stages and where A_{cca} has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$ and $\mathcal{D}_{sk_1}(\cdot)$. Note that* si *is the state information. It contains pk_0, pk_1, and so on. For* atk $\in$ {cpa, cca}*, we consider the following experiments:*

Experiment $\mathbf{Exp}^{\text{ik-atk-}b}_{\mathcal{PE},A_{\text{atk}}}(k)$
$I \leftarrow \mathcal{G}(k)$; $(pk_0, sk_0) \leftarrow \mathcal{K}(I)$; $(pk_1, sk_1) \leftarrow \mathcal{K}(I)$
$(x, \mathsf{si}) \leftarrow A^1_{\text{atk}}(pk_0, pk_1)$;
$y \leftarrow \mathcal{E}_{pk_b}(x)$;
$d \leftarrow A^2_{\text{atk}}(y, \mathsf{si})$
return d

Above it is mandated that A^2_{cca} never queries the challenge ciphertext y to either $\mathcal{D}_{sk_0}(\cdot)$ or $\mathcal{D}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantages via*

$$\mathbf{Adv}^{\text{ik-atk}}_{\mathcal{PE},A_{\text{atk}}}(k) = \left|\Pr[\mathbf{Exp}^{\text{ik-atk-1}}_{\mathcal{PE},A_{\text{atk}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{ik-atk-0}}_{\mathcal{PE},A_{\text{atk}}}(k) = 1]\right|.$$

The scheme $\mathcal{PE}$ is said to be IK-CPA secure (respectively IK-CCA secure) if $\mathbf{Adv}^{\text{ik-cpa}}_{\mathcal{PE},A_{\text{cpa}}}(\cdot)$ (resp. $\mathbf{Adv}^{\text{ik-cca}}_{\mathcal{PE},A_{\text{cca}}}(\cdot)$) is negligible for any adversary A whose time complexity is polynomial in k.

4.2 Encryption with Sampling Twice

In this section, we propose the encryption scheme with the sampling twice technique.

Definition 6. *The common-key generation algorithm $\mathcal{G}$ takes a security parameter k and returns parameters k, k_0, and k_1 such that $k_0(k)+k_1(k) < k$ for all $k > 1$. This defines an associated plaintext-length function $n(k) = k - k_0(k) - k_1(k)$. The key generation algorithm $\mathcal{K}$ takes k, k_0, k_1, runs the key-generation algorithm of* RSA*, and gets N, e, d. The public key pk is $(N, e), k, k_0, k_1$ and the secret key sk is $(N, d), k, k_0, k_1$. The other algorithms are depicted below. Let $G : \{0,1\}^{k_0} \to \{0,1\}^{n+k_1}$ and $H : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$ be hash functions. Note that $[x]^n$ denotes the n most significant bits of x and $[x]_m$ denotes the m least significant bits of x. Note that the valid ciphertext y satisfies $y \in [0, 2^k)$ and $(y \bmod N) \in \mathbb{Z}^*_N$.*

Algorithm $\mathcal{E}^{G,H}_{pk}(x)$
$r_1, r_2 \xleftarrow{R} \{0,1\}^{k_0}$
$s_1 \leftarrow (x||0^{k_1}) \oplus G(r_1)$; $t_1 \leftarrow r_1 \oplus H(s_1)$
$v_1 \leftarrow (s_1||t_1)^e \bmod N$
$s_2 \leftarrow (x||0^{k_1}) \oplus G(r_2)$; $t_2 \leftarrow r_2 \oplus H(s_2)$
$v_2 \leftarrow (s_2||t_2)^e \bmod N$
$y \leftarrow \texttt{ChooseAndShift}_{N,k}(v_1, v_2)$
return y

Algorithm $\mathcal{D}^{G,H}_{sk}(y)$
$v \leftarrow y \bmod N$
$s \leftarrow [v^d \bmod N]^{n+k_1}$; $t \leftarrow [v^d \bmod N]_{k_0}$
$r \leftarrow t \oplus H(s)$
$x \leftarrow [s \oplus G(r)]^n$; $p \leftarrow [s \oplus G(r)]_{k_1}$
if $(p = 0^{k_1})$ $z \leftarrow x$ **else** $z \leftarrow \perp$
return z

4.3 Analysis

We compare the four schemes with sampling twice, repeating, RSACD, and expanding.

4.3.1 Security

Bellare, Boldyreva, Desai, and Pointcheval [1] proved that the scheme with repeating (RSA-RAEP) is secure in the sense of IND-CCA2 and IK-CCA in the random oracle model assuming RSA is θ-partial one-way for $\theta > 0.5$. Hayashi, Okamoto, and Tanaka [6] proved that the encryption scheme with RSACD is also secure in the sense of IND-CCA2 and IK-CCA in the random oracle model assuming RSACD is θ-partial one-way for $\theta > 0.5$.

In order to prove that the scheme with sampling twice is secure in the sense of IK-CCA, we need the restriction as follows.

Since if c is a ciphertext of m for $pk = (N, e, k)$ and $c < 2^k - N$ then $c + N$ is also a ciphertext of m, the adversary can ask $c + N_0$ to decryption oracle $\mathcal{D}_{sk_0}$ where c is a challenge ciphertext such that $c < 2^k - N_0$ and $pk_0 = (N_0, e_0, k)$, and if the answer of $\mathcal{D}_{sk_0}$ is m, then the adversary can know that c was encrypted with pk_0.

To prevent this attack, we add some natural restriction to the adversaries in the definitions of IK-CCA. That is, it is mandated that the adversary never queries either $c' \in [0, 2^k)$ such that

	Sampling Twice	Repeating [1]	RSACD [6]	Expanding
# of mod. exp. to encrypt (average / worst)	2 / 2	1.5 / k_1	1.5 / 2	1 / 1
# of mod. exp. to decrypt (average / worst)	1 / 1	1 / 1	1.5 / 2	1 / 1
size of ciphertexts	k	k	k	$k+160$
# of random bits to encrypt (average / worst)	$2k_0+k+3$ / $2k_0+k+3$	$1.5k_0$ / k_1k_0	$1.5k_0$ / $1.5k_0$	k_0+160 / k_0+160

Figure 2: The comparison of the encryption schemes

$c' = c \pmod{N_0}$ to D_{sk_0} or $c'' \in [0, 2^k)$ such that $c'' = c \pmod{N_1}$ to D_{sk_1}.

Similarly, in order to prove that the scheme with sampling twice is secure in the sense of IND-CCA2, we need the same restriction. That is, in the definition of IND-CCA2, it is mandated that the adversary never queries $c' \in [0, 2^k)$ such that $c' = c \pmod{N}$ to D_{sk}.

We think these restrictions are natural and reasonable. Actually, in the case of undeniable and confirmer signature schemes, Galbraith and Mao [5] defined the anonymity on undeniable and confirmer signature schemes with the above restriction.

If we add these restrictions then we can prove that the scheme with sampling twice is secure in the sense of IK-CCA in the random oracle model assuming RSA is θ-partial one-way for $\theta > 0.5$. More precisely, we can prove the following theorem.

Theorem 2. *For any adversary A attacking the anonymity of our scheme Π under the adaptive chosen-ciphertext attack, and making at most q_{dec} decryption oracle queries, q_{gen} G-oracle queries, and q_{hash} H-oracle queries, there exists a θ-partial inverting adversary B for the* RSA *family, such that for any $k, k_0(k), k_1(k)$, and $\theta = \frac{k-k_0(k)}{k}$,*

$$\mathbf{Adv}^{\text{ik-cca}}_{\Pi,A}(k) \leq \frac{8q_{\mathrm{hash}}}{(1-\epsilon_1)\cdot(1-\epsilon_2)\cdot(1-\epsilon_3)} \cdot \mathbf{Adv}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},B}(k) + q_{\mathrm{gen}} \cdot q_{\mathrm{hash}} \cdot (1-\epsilon_3)^{-1} \cdot 2^{-k+2}$$

where $\epsilon_1 = \frac{1}{2}$, $\epsilon_2 = \frac{2}{2^{k/2-3}-1}$, $\epsilon_3 = \frac{2q_{\mathrm{gen}}}{2^{k_1}} + \frac{2q_{\mathrm{hash}}}{2^{k-k_0}} + \frac{2q_{\mathrm{gen}}+q_{\mathrm{dec}}+2q_{\mathrm{gen}}q_{\mathrm{dec}}}{2^{k_0}}$, and the running time of B is that of A plus $q_{\mathrm{gen}} \cdot q_{\mathrm{hash}} \cdot O(k^3)$.

Noticing that the range of valid ciphertexts changes, the proof is similar to that for RSA-RAEP and available in the full version [7].

We can also prove that the scheme with sampling twice is secure in the sense of IND-CCA2 in the random oracle model assuming RSA is θ-partial one-way for $\theta > 0.5$. More precisely, we can prove that if there exists a CCA2-adversary $A = (A_1, A_2)$ attacking indistinguishability of our scheme with advantage ϵ, then there exists a CCA2-adversary $B = (B_1, B_2)$ attacking indistinguishability of RSA-OAEP with advantage $\epsilon/2$. We construct B as follows.

1. B_1 gets pk and passes it to A_1. B_1 gets (m_0, m_1, si) which is an output of A_1, and B_1 outputs it.
2. B_2 gets a challenge ciphertext y and sets $y' \leftarrow y + tN$ where $t \stackrel{R}{\leftarrow} \{0,1\}$. If $y' \geq 2^k$ then B_2 outputs Fail and halts; otherwise B_2 passes (y', si) to A_2. B_2 gets $d \in \{0,1\}$ which is an output of A_2, and B_2 outputs it.

If B does not output Fail, A outputs correctly with advantage ϵ. Since $\Pr[B \text{ outputs Fail}] < 1/2$, the advantage of B is greater than $\epsilon/2$.

4.3.2 Efficiency

We show the number of modular exponentiations to encrypt, the number of modular exponentiations to decrypt, the size of ciphertexts, and the number of random bits to encrypt in Figure 2. We assume that N is uniformly distributed in $(2^{k-1}, 2^k)$.

5 Concluding Remarks

In this paper, we have proposed a new technique for obtaining the anonymity property of RSA-based cryptosystems, which we call "sampling twice." By applying the sampling twice technique, we have constructed the schemes for encryption, undeniable and confirmer signature, and ring signature.

For the comparison of the undeniable and confirmer signature schemes, in this paper, we only present the number of modular exponentiations to sign, the number of computation of square root, the size of signatures, and the number of random bits to sign in Figure 3. We assume that N is uniformly distributed in $(2^{k-1}, 2^k)$.

For ring signature, we present the number of modular exponentiations to sign, the number of modular exponentiations to verify, the size of signatures, and the number of random bits to sign in

	Sampling Twice	Expanding [5]	Repeating
# of mod. exp. to sign (average / worst)	2 / 2	1 / 1	1.5 / k_1
# of computation of square roots (average / worst)	2 / 2	1 / 1	1.5 / k_1
size of signatures	$k + k_0$	$2k + k_0$	$(k-1) + k_0$
# of random bits to sign (average / worst)	$k_0 + k + 5$ / $k_0 + k + 5$	$k_0 + k + 2$ / $k_0 + k + 2$	$1.5(k_0 + 2)$ / $k_1(k_0 + 2)$

Figure 3: The comparison of the undeniable and confirmer signature schemes

	Sampling Twice	Expanding [8]	RSACD [6]	Repeating
# of mod. exp. to sign (average / worst)	$2r$ / $2r$	r / r	$1.5r$ / $2r$	$1.5r$ / kr
# of mod. exp. to verify (average / worst)	r / r	r / r	$1.5r$ / $2r$	r / r
size of signatures	$(3r+1)k + r$	$(3r+1)k + 160(r+1)$	$(3r+1)k$	$(3r+1)k - 1$
# of random bits to sign (average / worst)	$3(k+1)(r-1) + k$ / $3(k+1)(r-1) + k$	$(k+160)r$ / $(k+160)r$	kr / kr	$1.5k(r-1) + k - 1$ / $k^2(r-1) + k - 1$

Figure 4: The comparison of the ring signature schemes ($|N_i| = k$)

Figure 4. We assume that each N_i is uniformly distributed in $(2^{k-1}, 2^k)$.

Due to lack of space, details have been omitted from this paper. See the full version [7].

In our analysis, we have observed that the scheme with sampling twice is efficient with respect to the sizes of ciphertexts and signatures, the computational costs to decrypt ciphertexts and to verify signatures in the average and worst cases, and the computational costs to encrypt messages and to sign messages in the worst case.

References

[1] Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In Boyd [2], pp. 566–582. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir/`.

[2] Boyd, C., Ed. *Advances in Cryptology - ASIACRYPT 2001* (Gold Coast, Australia, December 2001), vol. 2248 of *Lecture Notes in Computer Science*, Springer-Verlag.

[3] Desmedt, Y. Securing traceability of ciphertexts: Towards a secure software escrow scheme. In *Advances in Cryptology - EUROCRYPT '95* (Saint-Malo, France, May 1995), L. C. Guillou and J.-J. Quisquater, Eds., vol. 921 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 147–157.

[4] Fujisaki, E., Okamoto, T., Pointcheval, D., and Stern, J. RSA-OAEP is Secure under the RSA Assumption. In *Advances in Cryptology - CRYPTO 2001* (Santa Barbara, California, USA, August 2001), J. Kilian, Ed., vol. 2139 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 260–274.

[5] Galbraith, S. D., and Mao, W. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In *Topics in Cryptology - CT-RSA 2003* (San Francisco, CA, USA, April 2003), M. Joye, Ed., vol. 2612 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 80–97.

[6] Hayashi, R., Okamoto, T., and Tanaka, K. An RSA Family of Trap-door Permutations with a Common Domain and its Applications. In *Public Key Cryptography - PKC 2004* (Singapore, March 2004), F. Bao, R. H. Deng, and J. Zhou, Eds., vol. 2947 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 291–304.

[7] Hayashi, R., and Tanaka, K. The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity. Research Report C-201, Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology, `http://www.is.titech.ac.jp/research/research-report/`, December 2004.

[8] Rivest, R. L., Shamir, A., and Tauman, Y. How to Leak a Secret. In Boyd [2], pp. 552–565.